United Kingdom

Data Protection Implications of 'Brexit'

*Lokke Moerel and Ronan Tigner**

The population of the United Kingdom has voted by a narrow majority to leave the European Union (Brexit). But the process of Brexit will take time, and the implications for companies will also unfold over time.

I. No Changes in the Short Term

For the time being, the UK remains a member of the EU and the EU Data Protection Directive 95/46/EC (the Directive) and e-Privacy Directive (2002/58/EC) as currently implemented in UK law continue to apply. The Directive will be replaced by the EU General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) in May 2018, and in the coming period the e-Privacy Directive will be updated to reflect the changes that the GDPR will bring. Given the time that will elapse before Brexit actually occurs, it may well be the case that the GDPR will come into force before the UK formally exits the EU.

As the GDPR has the form of an EU Regulation, it will be directly applicable in all EU Member States, and no steps need to be taken by the UK for it to be implemented in its national laws. Further, it may well be the case that the UK will have to implement the amended e-Privacy Directive into UK law before Brexit takes place. Until the UK formally exits the EU, data transfers between the UK and the other countries in the EU may continue to occur without changes because the EU data transfer rules do not apply to transfers of personal data within the EU.

II. Changes after Brexit

The situation will change when the UK leaves the EU. From that moment on, the GDPR will no longer be applicable in the UK. The national laws implementing EU Directives (including the e-Privacy Directive) will, however, remain in force until they are amended or repealed. Thus, the UK will become a 'third country' under the data transfer rules in the GDPR. As a result personal data can only be exported by a business established in the EU to a third country, such as the UK, if there is an 'adequate level of protection' for such data, unless certain conditions have been met.

There are three options under which the UK may obtain the required 'adequacy status', with the third being the most likely:

- *Becoming an EEA member:* The UK may (like Norway, Liechtenstein and Iceland) become a member of the European Economic Area (EEA) by becoming a signatory to the EEA Agreement[1]. Under Article 7 of the EEA Agreement, the UK would still need to accept being bound directly by relevant EU laws relating to the four freedoms, including the GDPR. This option is unlikely to be pursued by the UK government in the form adopted by Norway, Liechtenstein and Iceland, in view of the fact that the UK would need to agree to be bound by many of the rules of the EU which have been unpopular with Brexit supporters, including the free movement of people.
- *The Swiss solution:* Switzerland is not part of the EU or EEA (although it has bilateral agreements with the EU allowing access to the single market). Although not bound by it, Switzerland has fully implemented the Directive into its domestic legislation and, on this basis, has received an 'adequa-

* Prof. Lokke Moerel is a senior of counsel at global law firm Morrison & Foerster; for correspondence: <LMoerel@mofo.com>. Ronan Tigner is an associate at Morrison & Foerster; for correspondence: <RTigner@mofo.com>.

1 Agreement on the European Economic Area, OJ EC L 1 of 3 January 1994, 3. Consolidated version available at <http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf> accessed 13 September 2016.

cy finding' from the European Commission. Switzerland has already indicated its wish to update Swiss legislation to reflect the application of the GDPR and retain its adequacy status. Also, although Switzerland is not subject to the jurisdiction of the Court of Justice of the European Union (CJEU), the CJEU's case law has had a significant influence on the Swiss legal regime. For instance, after the CJEU struck down the EU-US Safe Harbour Decision of the Commission in the *Schrems* judgment[2], the Swiss also declared that the Swiss-US Safe Harbour did not provide a sufficient legal basis for exporting data from Switzerland to the US. As with becoming a member of the EEA, the Swiss model would require the UK to adopt the GDPR as it stands now and any further EU legislation on data protection, without having any right to participate in EU rule-making. This option is unlikely to be pursued by the UK government in the form adopted by Switzerland because it would again entail the UK agreeing to be bound by many of the rules of the EU which have been unpopular with Brexit supporters.

- *Full adequacy finding:* The UK implements its own data protection laws and requests the Commission to issue a decision that its legal regime is 'adequate' when assessed against the standard set by EU data protection law. At first sight, this seems the preferred option because it enables the UK to relax some of the rules in order to facilitate trade (as it advocated in the negotiations over the GDPR). However, if the UK wishes to obtain a quick adequacy decision to continue to facilitate data transfers between the UK and the EU also upon exit, it will likely have to implement provisions that are close to the GDPR. The EU may well be averse to any softening of the rules that would give the UK an advantage over EU Member States, or enable some sort of forum shopping. It is therefore not surprising that the UK Information Commissioner's Office (ICO) has already issued a statement that UK data protection standards would have to be *equivalent* to the GDPR. We note that the UK has been a long-standing advocate of data protection (eg, it had a law more than 10 years before the Directive was adopted) and there is solid public awareness of privacy laws. The UK has further ratified Convention 108 (which sets core principles for data protection) as well as the European Convention on Human Rights (ECHR – which, in Article 8, provides for the right to privacy), and the UK is subject to the European Court of Human Rights' competence. The ICO is a member of the Global Privacy Enforcement Network (GPEN), intended to strengthen cross-border information sharing and enforcement among privacy authorities around the world. This all seems to point into the direction of adequacy. We highlight, however, that the recent *Schrems* judgment of the CJEU may also have implications for the UK. In the *Schrems* judgment, the CJEU invalidated the decision of the Commission that approved the Safe Harbour Framework facilitating data transfer to US companies that adhered to this framework, because the privacy of European citizens was not considered to be adequately protected (in short) because the powers of the U.S. intelligence services went beyond what was strictly necessary and proportionate to the protection of national security and individuals did not have adequate means of judicial redress to protect their privacy. The concern that the intelligence services have overly broad surveillance powers may well also apply to the UK intelligence services.[3] More clarity may come from three cases pending before the European Court of Human Rights, which were instigated by the UK Bureau of Investigative Journalism and a number of civil rights organisations, and claim that the generic surveillance powers of the UK intelligence services violate Article 8 of the ECHR.[4]

III. Next Steps for Businesses

While it is expected that the Commission will eventually confirm 'adequacy status' for the data protection laws the UK puts in place post-Brexit, it is pos-

2 Case C-362/14 *Schrems* (CJEU, 6 October 2015) ECLI:EU:C:2015:650; cf Neal Cohen, 'The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework – Case C-362/14, Schrems' (2015) 3 EDPL 240.

3 Cf on the reform of these powers, as laid down in the Regulation of Investigatory Powers Act (RIPA), Lorna Woods, 'Draft Investigatory Powers Bill' (2016) 1 EDPL 103.

4 *Big Brother Watch & Ors v United Kingdom* App no 58170/13 (ECtHR); *Bureau of Investigative Journalism & Ors v United Kingdom* App no 62322/14 (ECtHR); *10 Human Rights Organisations & Ors v United Kingdom* App no 24960/15 (ECtHR). Cf on these proceedings Sebastian Schweda, 'UK Surveillance Under Judicial Scrutiny: GCHQ Intelligence Sharing with NSA Contravened Human Rights, But Is Now Legal' (2015) 1 EDPL 61.

sible that this may not have been done at the precise time of exit. This situation would require businesses to put in place alternative data transfer arrangements for transfers from within the EU to the UK, such as the entering into standard contractual clauses (SCCs). Controllers and processors can also 'adduce appropriate safeguards' for their intra-group transfers by adopting binding corporate rules (BCRs). In any case, in the aftermath of the *Schrems* judgment, we see a trend of companies moving to implement BCRs in order to be less dependent on the adequacy decisions of the Commission and the negotiations of the EU and US in respect of the terms of the new Privacy Shield.

Given the lead time it takes to implement the GDPR requirements into business processes, the advice to businesses in the UK is to continue their GDPR readiness programmes. As indicated above, the rules that the UK will ultimately implement in all likelihood will closely resemble the GDPR. Note further that the GDPR may continue to apply to the data processing activities of UK companies where they offer goods or services to citizens in other EU countries, or otherwise monitor their behaviour. The same will apply to UK companies with offices in other EU countries operating central data processing systems.

The ICO has acted as the lead data protection authority (DPA) in approving BCRs in many instances. After the exit, the ICO will no longer be authorised to act as lead DPA. Companies with BCRs where the ICO is lead DPA will therefore have to approach another EU DPA to act as their lead DPA. Businesses applying for BCRs and having to select a lead DPA and co-leads should be advised to take this into account.